STATE OF VERMONT
Agency of Administration

POLICY MANUAL IRMAC INFORMATION RESOURCE MANAGEMENT ADVISORY COUNCIL	ORIGINAL POLICY ADOPTED BY IRMAC DATE: 10/08/02	ORIGINAL POLICY NUMBER
	EFFECTIVE DATE 10/08/02	IDENTIFIER

STATUTORY REFERENCE OR OTHER AUTHORITY: **IRMAC Resolution**

APPROVAL DATE: 10/08/02

APPROVED BY:

POLICY TITLE: **Security Risk Assessment**

POLICY STATEMENT:

A Security Risk Assessment is a process to ensure that the security controls for a system are appropriate when compared to its acceptable risks. The goal of a Security Risk Assessment is to objectively and meticulously evaluate the relative importance of all threats and vulnerabilities, and generate appropriate solutions and recommendations. It should also automatically link the risks identified with the potential implications for the business unit.

Security Risk Assessments may be conducted on any entity connected to GOVnet or any outside entity that has signed a *Third Party Agreement* with an Agency/Department under the direction of the Office of the CIO and with cooperation of Agencies/Departments being assessed. Security Risk Assessments can be conducted on any information system, physical security, and any process or procedure by which these systems are administered and/or maintained. Security Risk assessments that attempt to penetrate secure facilities, physically, electronically, or by means of social engineering, can only be conducted under the direction of the Office of the CIO. The Appointing Authority of the entity being assessed is expected to provide appropriate resources to cooperate fully with any risk assessment being conducted on systems for which they are held accountable.

Security Risk Assessments teams may include third party vendors contracted by the State, state personnel, or any combination thereof and are generally referred to as Tiger teams—a group of individuals who legitimately attempt to compromise a set of security measures put in place by the employer to find weaknesses in the employer's security. Assessment team members are required to accept and sign any and all non-disclosure and or confidentiality agreements required by the Agencies/Departments being assessed before assessment can begin. Results of the assessment are protected under Title 1 Chapter 5, §317(25). These results contain extremely sensitive material regarding the state's security measures and will only be distributed to the Office of the CIO, and the head of the Agency/Departments being assessed, and may, as necessary, be distributed to Vermont CSIRT for the purposes of remediation.

The execution, development and implementation of remediation programs is the joint responsibility of the Office of the CIO, Vermont CSIRT, and the department responsible for the systems area being assessed.

The risk assessment may be triggered by any of the following conditions:

- ?? Recommendation by the Office of the CIO
- ?? Request by a Agency/Department
- ?? Request by the Vermont CSIRT
- ?? Security breach of an internal system
- ?? New enterprise application
- ?? Training exercise

PURPOSE/COMMENT: To empower the Office of the CIO to coordinate periodic information Security Risk Assessments for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.